UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/711,028	11/09/2000	Joseph Wayne Freeman	RPS920000043US1	6737

7590 07/16/2004

BRACEWELL & PATTERSON, L.L.P.
INTELLECTUAL PROPERTY LAW
P.O. BOX 969
AUSTIN,, TX 78767-0969

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/711,028	FREEMAN ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Novoa et al(6,223,284).

3. As per claim 1, Novoa et al.(6,223,284) discloses a method of enabling use of a secure password(see col. 3, lines 10-13) , during power up initialization before an operating system is started(see col. 3, lines 13-15), copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system; and before starting the operating system, hard locking the memory device against direct access so that a reset signal is required to unlock the memory device(see col. 3, lines 13-25, col. 13, lines 19-44).

4. As per claim 2, Novoa et al. discloses responsive to receiving an entered password under the operating system(see col. 22, lines 30-35), calling a routine executing within the restricted portion of system memory to verify the password(see col. 22, lines 33-37); and receiving an indication from the routine regarding whether the entered password matched a password within the security data copied to the restricted portion of system memory from the memory device(see col. 27, lines 6-23).

5. As per claim 3, Novoa et al. discloses wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprises: checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine(see col. 27, lines 5-23).

6. As per claim 4, Novoa et al. discloses wherein the step of checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine includes placing a label within a basic input/output services routine implementing a process for copying the security data immediately after instruction(see col. 3, lines 10-40); for the call requesting that the security data be copied; placing an address for the label within code executing within the restricted portion of system memory and checking the return address for the call requesting that the security data be copied(see col. 3, lines 10-26, col. 6 lines 31-51); comparing the return address and the address for the label; responsive to determining that the return address does not match the address for the label, returning a null response to the call requesting that the security data be copied; and responsive to determining that the return address matches the address for the label, copying the security data to the restricted portion of system memory and resetting a retry counter(see col. 3, lines 26-41, col. 9, lines 1-48).

5. As per claim 5, Novoa et al. discloses wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system further comprises: copying the password and other sensitive data which requires protection from access under the operating system(see col. 3, lines 10-25).

6. As per claim 6, Novoa et al. discloses wherein the step of copying security data from a memory device to a restricted portion of system memory which is invisible to the operating system includes loading the security data to regular system memory prior to initiating the call requesting that the security data be copied(see col. 3, lines 10-26); and upon receiving any response to the call requesting that the security data be copied, erasing the security data from regular system memory before starting the operating system(see col. 3, lines 26-41).

7. As per claim 7, Novoa et al. discloses a method of enabling use of a secure password, responsive to receiving an entered password under an operating system(see col. 3, lines 10-13), calling a routine executing within a restricted portion of system memory to verify the password, wherein the restricted portion of system memory is invisible to the operating system and wherein the operating system and routines executing within the restricted portion of system memory communicate through a calling convention(see col. 22, lines 30-55); and receiving only an indication from the routine executing within the restricted portion of memory regarding whether the entered password matched a password stored within the restricted portion of system memory(see col. 22, lines 33-41).

8. As per claim 8, Novoa et al. discloses during power up initialization before the operating system is started, copying a password from a memory device to the restricted portion of system memory; and before starting the operating system, hard locking the memory device against direct access so that a reset signal is required to unlock the memory device(see col. 22, lines 7-55).

9. As per claim 9, Novoa et al. discloses determining whether a password is required for an operation by checking with the routine executing within a restricted portion of system memory to verify existence of a password(see col. 3, lines 10-41).

10. As per claim 10, Novoa et al. discloses limiting a number of retries for a user to reenter a password(see col. 6, lines 31-51).

11. As per claim 11, Novoa et al. discloses transmitting the entered password entered by a user to the routine executing within a restricted portion of system memory using the calling convention(see col. 26, lines 52-67; and responsive to receiving an indication from the routine executing within the restricted portion of memory that the entered password matched the password stored within the restricted portion of system memory, continuing an operation requiring the entered password for execution(see col. 27, lines 6-23).

12. As per claim 12, Novoa et al. discloses a data processing system, comprising: a memory device which may be hard locked against direct access so that a reset signal is required to unlock the memory device(see col. 27, lines 6-10); and a power up initialization routine executing within the data processing system, wherein the power up initialization routine, before starting an operating system, copies security data from the memory device to a restricted portion of system memory which is invisible to the operating system and hard locks the memory device(see col. 3, lines 10-26).

13. As per claim 13, Novoa et al. discloses wherein the power up initialization routine, responsive to receiving an entered password under the operating system(see col. 3, lines 10-12), calls a routine executing within the restricted portion of system memory

to verify the password and receives an indication from the routine regarding whether the entered password matched a password within the security data copied to the restricted portion of system memory from the memory device(see col. 3, lines 13-41).

14. As per claim 14, Novoa et al. discloses wherein the routine executing within the restricted portion of system memory checks a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine(see col. 3, lines 10-41).

15. As per claim 15, Novoa et al. discloses wherein the power up initialization routine, to facilitate checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine(see col. 3, lines 13-41), places a label within a basic input/output services routine implementing a process for copying the security data immediately after instruction; for the call requesting that the security data be copied, wherein the routine executing within the restricted portion of system memory contains an address for the label(see col. 6, lines 31-51), checks the return address for the call requesting that the security data be copied, and compares the return address and the address for the label and, responsive to determining that the return address does not match the address for the label(see col. 7, lines 2-19), returning a null response to the call requesting that the security data be copied, and responsive to determining that the return address matches the address for the label, copying the security data to the restricted portion of system memory and resetting a retry counter(see col. 22, lines 30-55).

16. As per claim 16, Novoa et al. discloses wherein the power up initialization routine copies the password and other sensitive data which requires protection from access under the operating system(see col. 3, lines 10-26).

17. As per claim 17, Novoa et al. discloses wherein the power up initialization routine loads the security data to regular system memory prior to initiating the call requesting that the security data be copied and(see col. 3, lines 10-26), upon receiving any response to the call requesting that the security data be copied, erases the security data from regular system memory before starting the operating system(see col. 3, lines 27-41).

18. As per claim 18, Novoa et al. discloses an operating system; a memory device which may be hard locked against direct access so that a reset signal is required to unlock the memory device(see col. 27, lines 6-10); a system memory including a restricted portion invisible to the operating system(see col. 3, lines 10-41), wherein the operating system and routines executing within the restricted portion of system memory communicate through a calling convention; and a power up initialization routine executing within the data processing system(see col. 3, lines 10-41), wherein the power up initialization routine, responsive to receiving an entered password under an operating system, calls a routine executing within a restricted portion of system memory to verify the password(see col. 3, lines 27-41), and receives only an indication from the routine executing within the restricted portion of memory regarding whether the entered password matched a password stored within the restricted portion of system memory(see col. 3, lines 30-55).

19. As per claim 19, recites limitations already addressed(see claim 8).

20. As per claim 20, recites limitations already addressed(see claim 9).

21. As per claim 21, recites limitations already addressed(see claim 10).

22. As per claim 22, recites limitations already addressed(see claim 11).

23. As per claim 23, Novoa et al. discloses a computer program product within a computer usable medium for enabling use of a secure password, instructions for copying security data from a memory device to a restricted portion of a system memory which is invisible to the operating system during power up initialization before an operating system is started(see col. 27, lines 6-10); and instructions for hard locking the memory device against direct access so that a reset signal is required to unlock the memory device before starting the operating system(see col. 3, lines 10-26).

24. As per claim 24, limitations already addressed(see claim 13).

25. As per claim 25, limitations already addressed(see claim 3).

26. As per claim 26, limitations already addressed(see claim 4).

27. As per claim 27, limitations already addressed(see claim 5).

28. As per claim 28, limitations already addressed(see claim 6).

29. As per claim 29, limitations already addressed(see claim 7).

30. As per claim 30, limitations already addressed(see claim 8).

31. As per claim 31, limitations already addressed(see claim 9).

32. As per claim 32, limitations already addressed(see claim 10).

33. As per claim 33, limitations already addressed(see claim 11).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

July 7, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100